Security Architecture Work Group

Monday March 25, 2002
10:00 A.M. to Noon
NSOB LLC -- Lincoln

Minutes

A. Participants

Allan	Albers	HHSS
Mahendra	Bansal	Dept of Natural Resources
Jason	Everett	ESU 10, Kearney (via conference call)
Jerry	Hielen	IMServices
Dennis	Linster	Wayne State College (via conference call)
Scott	McFall	Nebraska State Patrol
Jon	Ogden	Department of Roads
Steve	Rathje	Dept of Natural Resources
Steve	Schafer	Nebraska CIO
Ron	Woerner	Department of Roads

B. Incident Response and Reporting

Steve Schafer asked for further advice regarding the draft procedures. So far, no agencies have reported incidents using an earlier draft of the procedures that was distributed last October. The revised draft includes an abbreviated one-page form for reporting incidents. It also clarifies the types of incidents that should be reported. Both changes reflect a reporting policy developed in conjunction with the FBI, Secret Service and CIO Magazine.

Suggestions included adding a flow chart that shows the incident response process and including "inappropriate use by employees" as one of the types of incidents on the reporting form. Another change is to include external contacts for reporting purposes (FBI, State Patrol, and CIO).

Discussion emphasized the importance of management support for documenting incidents and sharing that information with external entities. The justification includes identifying trends, patterns, and possible forensic use.

C. Agency Security Planning

1. Department of Roads

   Ron Woerner (Information Security Officer for DOR) gave an overview of their activities. These include:
   - (1) Forming a security advisory team of technical staff to serve as a sounding board;
   - (2) Management involvement in approving policies;
   - (3) Close coordination with the human resource division;
   - (4) Developing a limited number of policies, with specific standards and guidelines;

   Future efforts will focus on an awareness program, including training for new hires and posting security information on DOR's intranet site. One aspect of awareness is promoting a sense of responsibility for one's computer account and the need for a strong password. DOR will provide

1

advice to employees on setting up passwords. DOR is also working on a remote user access policy. It will require measures such as virus protection and firewalls for home users.

Another effort is working on a business impact analysis. This will be helpful for disaster recovery planning as well as security planning. It also impacts data classification and security requirements for data. DOR is investigating the feasibility of including a hot site in the proposed Joint Operation Center.

DOR is working with the Peter Kiewit Institute to arrange for an intern to help with conducting vulnerability assessments.

2. Health and Human Services
Alan Albers (security administrator for HHS) has been assigned to work exclusively on security issues since January. His current focus is an audit by the IRS. He is forming a security advisory team with a mix of technical and business expertise. The group will help prepare written security policies and procedures. A risk assessment of CHARTS and associated hardware is required for PRWORA certification. Alan is using the templates from the security handbooks. By November or December, Alan hopes to incorporate a security training process into new employee orientation. This is required by HIPAA.

Other activities include working on secure e-mail options with the Office of the CIO and other agencies. HHS also implemented Citrix as an inexpensive option for providing county attorneys access to CHARTS. This saves the cost of dedicated lines.

D. **Security Procedures Documentation Update**
(Latest versions of the templates are available at: http://www.nitc.state.ne.us/tp/workgroups/security/index.htm).

Jerry Hielen gave an overview of current activities. Since last fall, IMServices has developed a set of work papers for conducting a risk analysis and a glossary of terms. Both are available on the web site (see above

E. **Update on Other Security Initiatives**
1. Enterprise Security Awareness Training
(http://www.nitc.state.ne.us/sgc/grants/2001/gtcf2001awards.htm)
IMServices is also working on the training awareness project, which is partially funded by a Government Technology Collaboration Fund grant. The training will be targeted to security officers and technical staff. To address the training needs of general users, IMServices is investigating a web-based training module from CorpNet in Omaha. (Alan Albers noted that HHS is using a similar product called Smartforce.)

2. IMServices Security and Directory Services Study (project check point)
The security directory is another project. It would provide an enterprise solution for authentication. Eventually, it would replace the custom application named Guardian and would include features such as user self-registration and role and policy-based security. Phase I of the security directory study was completed several months ago. Phase II is now underway. It will determine the detailed requirements of agencies relating to authentication.

F. Security Assessment RFP   (http://www.nitc.state.ne.us/sgc/grants/2001/gtcf2001awards.htm)
Discussion included the following points:

- The IRS security requirements impact both HHS and Revenue. Their standards include a requirement for a security assessment (IRS 1075 . The IRS is moving toward a "common criteria" set of security standards.
- A separate group rather than the Security workgroup should help with developing the RFP and selecting a vendor.
- All agencies that might be affected should be notified ahead of time about the security assessment.
- The security assessment will include Nebraska Online.
- A statement from the CIO to affected agencies should explain that the purpose of the assessment is a learning exercise.

G. Other Implementation Issues
1. Disaster recovery and business continuity
2. Business Case Outline
3. Security web site (http://www.nitc.state.ne.us/tp/workgroups/security/index.htm)
4. Other topics

H. Next Meeting Date